PUBLIC KEY CRYPTOGRAPHIC APPARATUS AND METHOD

ABSTRACT OF THE DISCLOSURE

A method and apparatus are disclosed for improving public key encryption and decryption schemes that employ a composite number formed from three or more distinct primes. The encryption or decryption tasks may be broken down into sub-tasks to obtain encrypted or decrypted sub-parts that are then combined using a form of the Chinese Remainder Theorem to obtain the encrypted or decrypted value. A parallel encryption/decryption architecture is disclosed to take advantage of the inventive method.